



UNITED STATES
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

October 2, 2003

The Honorable Edward J. Markey
United States House of Representatives
Washington, D.C. 20515

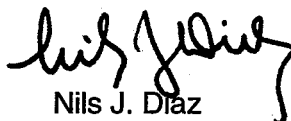
Dear Congressman Markey:

On behalf of the Nuclear Regulatory Commission (NRC), I am responding to your letter dated August 22, 2003, concerning the Microsoft SQL Server computer worm known as "Slammer." You asked questions about the impact that this worm might have had on the computer systems at the Davis-Besse Nuclear Power Plant and, more generally, about the protections against cyber attack that are available at NRC-licensed nuclear power plants.

The NRC has taken an aggressive stance on security at nuclear facilities, both before and since the terrorist events of September 11, 2001. The enhancements that the NRC has required have bolstered security at nuclear power plants in many areas, including specific actions to address cyber security. The NRC is in the process of inspecting licensed facilities and activities to ensure compliance with the requirements mandated by the NRC and will analyze the findings from these inspections to determine what actions are appropriate. No cyber vulnerabilities have been identified which would affect the safe operation of the plants. With respect to Davis-Besse, the Microsoft SQL Server worm did not infect systems that are important to nuclear safety. Additionally, it should be noted that Davis-Besse was in a safely defueled condition at the time of the event.

I am providing more detailed answers to your questions in the enclosure. If you have further questions, please contact me.

Sincerely,



Nils J. Diaz

Enclosure: Questions and Answers

cc: The Honorable Spencer Abraham, Secretary
U.S. Department of Energy
The Honorable Tom Ridge, Secretary
U.S. Department of Homeland Security
The Honorable Pat Wood, Chairman
Federal Energy Regulatory Commission
Michehl Gent, President
North American Electricity Reliability Council

Question 1: What proposals has the NRC made to strengthen its cyber-security regulations since September 11, 2001? If no such changes were made, why not?

Answer: The NRC has taken steps to enhance security at its licensed facilities since September 11, 2001, including the area of cyber security. On October 6, 2001, the NRC issued a safeguards advisory that described prompt and additional actions that should be taken by the licensees. On February 15, 2002, another safeguards advisory was issued concerning the Simple Network Management Protocol, Version 1, a "backbone" program for networking devices. This advisory mirrored another such communication from the National Infrastructure Protection Center, and was modified slightly to address specific areas for NRC licensees.

On February 25, 2002, the NRC issued Orders to nuclear power plant licensees concerning enhancements to security. On April 29, 2003, another Order was issued to licensees revising the design basis threat (DBT) and requiring licensees to modify their physical security systems to protect against that threat. Cyber security was addressed in both orders.

In October 2002, the NRC initiated a cyber assessment project to develop a cyber security self-assessment methodology for nuclear power plant licensees to use in evaluating their systems for potential cyber vulnerabilities. As part of this process, the NRC has conducted pilot studies at four nuclear power plants using a baseline method developed by NRC and Pacific Northwest National Laboratories (PNNL) in conjunction with the Nuclear Energy Institute (NEI) and industry. The NRC staff is also involved in the development of a comprehensive cyber security assessment program guideline to be issued by NEI. This guideline would incorporate the NRC-developed methodology and provide guidance to licensees for self-assessment of their plants' cyber vulnerabilities and implementation of necessary mitigating measures. Once the plan is endorsed by the NRC, it will be implemented by power reactor licensees.

Question 2: Was First Energy in violation of NRC's cyber-security regulations when the Davis-Besse plant was penetrated by the Slammer worm? If so, what penalty did the NRC impose?

Answer: First Energy was not in violation of NRC's requirements when the Davis-Besse plant was penetrated by the Microsoft SQL Server worm, known as "Slammer." During this event, some systems used by the operations staff were temporarily unavailable, including the Safety Parameter Display System (SPDS) and the Plant Process Computer (PPC). Neither of these systems affect the safety of the facility but assist the operators in monitoring plant parameters. Although the operators were burdened by the unavailability of these systems, the event was not deemed significant since the plant control and protection functions were not affected.

Question 3: What proposals has the NRC made to strengthen its cyber-security regulations since the Slammer worm penetrated the Davis-Besse plant in January 2003? If no such changes were made, why not, since the incident clearly highlighted a serious and exploitable problem?

Answer: See response to question 1, above. In addition, on August 29, 2003, the NRC issued Information Notice 2003-14, "Potential Vulnerability of Plant Computer Network to Worm Infection," (copy attached) to power reactor licensees to alert them to the events surrounding the Davis-Besse infection. Licensees are expected to review the information for applicability to their facilities and to consider taking action as appropriate. Following NRC review of the results from the four pilot studies, NRC will determine whether any additional regulatory action is appropriate.

Question 4: Please provide copies of all cyber-security reviews the NRC has performed on individual reactors or industry-wide since September 11, 2001. If no such review have been performed, why not?

Answer: The NRC inspection reports that reviewed implementation of the February 25, 2002, Orders included a section on cyber security. Due to the sensitive nature of this information, the appropriate portions of those reports are being forwarded under separate cover.

Question 5: Has the NRC inspected the cyber-security measures taken by other nuclear reactors in order to determine whether they are in compliance with NRC regulations? If so, what was the result? If not, why not?

Answer: The reports from the four pilot studies have not yet been completed. The pilot studies, which included attempts to penetrate the systems, identified some common vulnerabilities relating to the network architecture but these vulnerabilities did not involve safety systems or safety-related systems.

Question 6: Does the NRC ever conduct tests of the adequacy of cyber-security at nuclear power plants? How often? How many plants have been tested, and what were the results? Do these tests consist of NRC attempts to penetrate the plants' networks in order to determine whether hackers, a virus or a cyber-terrorist could do so?

Answer: See responses to questions 1 and 5, above.

Question 7: Is there any evidence that last week's blackout could have been caused by the Blaster worm or some other cyber-security flaw? If so, please provide it.

Answer: The NRC has no information that the recent blackout of the northeastern portion of the United States was caused by the Blaster worm or other cyber-security flaw.

Question 8: Do you believe it is possible that a cyber-attack could successfully penetrate nuclear reactor networks and result in an outage of that reactor and/or a more widespread outage? Why or why not?

Answer: The NRC is currently evaluating this set of circumstances to determine the impact on plant operations. The ongoing assessment program and related inspection activities will inform decisions made by the NRC in this area.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, DC 20555-0001

August 29, 2003

NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT
COMPUTER NETWORK TO WORM INFECTION

Addressees

All holders of operating licenses for nuclear power reactors, except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.

Purpose

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice to alert addressees to the recent identification of a potential vulnerability of the plant computer network server to infection by the Microsoft (MS) SQL Server worm. The NRC anticipates that recipients will review the information for applicability to their facilities and consider taking appropriate actions to prevent the MS SQL Server worm from infecting their plant network servers. However, suggestions contained in this information notice are not NRC requirements; therefore, no specific action or written response is required.

Background

Microsoft (MS) SQL Server 2000 is a database software program for network servers. The program contains a remotely exploitable stack buffer overflow that is vulnerable to potential hackers. When an overflow occurs, arbitrary code can be executed on the victim system with the user privileges of the SQL Server. Once a server is compromised, the MS SQL Server 2000 Worm propagates itself by making packets of 376 bytes and sending them to randomly chosen Internet Protocol (IP) addresses User Datagram Protocol (UDP) port 1434. If the packet is sent to a vulnerable machine, the machine becomes infected and begins to propagate. This worm activity is readily identifiable on the computer network by the presence of 376-byte UDP packets. Microsoft Corporation identified this vulnerability in the SQL Server 2000 and issued a security patch on July 10, 2002. When Microsoft Corporation releases a patch to fix a problem for its software, the full details of the vulnerability of the product are disclosed.

Description of Circumstances

On January 25, 2003, Davis-Besse nuclear power plant was infected with the MS SQL Server 2000 worm. The infection caused data overload in the site network, resulting in the inability of the computers to communicate with each other. The slowness in computer processing speed began in the morning and by 4:50 p.m., the Safety Parameter Display System (SPDS) became

ML032410430

Attachment

unavailable and remained unavailable for 4 hours 50 minutes. By 5:13 p.m., the plant process computer was lost and remained unavailable for 6 hrs and 9 minutes. Although the operators were burdened by these losses, the event was not deemed significant since the plant control and protection functions were not affected.

Because the MS SQL worm resided in only memory, shutting down the server removed the worm from the server's memory, ridding the server of the infection. The licensee isolated the server from the site network, installed the MS security patch, and reconnected the server to the site network.

Discussion

First Energy Nuclear's (the licensee's) corporate network, which is linked with Davis-Besse's plant network, is connected to external networks via a firewall. A firewall is a system or systems that enforce an access control policy between networks. Among the many access control policies that Davis-Besse's corporate firewall enforced was the policy of disallowing any data using the UDP into the network by closing port 1434 of the firewall. This policy would have protected Davis-Besse's networks from the MS SQL worm infection except that the corporate network had a T1 connection behind the firewall that provided a path for the worm to enter the system. This T1 line was used by one of the licensee's consultants who provided an application software that ran on a server. This connection bypassed all the access control policies that the corporate firewall was enforcing, including the policy of preventing data that used the UDP from coming into the corporate network.

The consultant's company network server allowed use of the UDP for data transfers and was infected by the MS SQL worm. When the consultant established a T1 line connection at the licensee's corporate site, this action opened a path by which the worm that infected the consultant's company server was sent to the licensee's corporate network through the T1 line. The worm then randomly infected any servers on the corporate network that had port 1434 open.

Two primary causes for this worm infection were noted:

1. The T1 connection behind the firewall

The corporate network would not have been infected by the worm if the consultant's T1 line had been connected in front of the firewall. In February 2002, the NRC issued a security order which alerted licensees to external connections that bypass network protective measures. Subsequent to this event, the licensee noted that the implementation of the order was addressed by the Information Technology personnel; however, their activities were not communicated to the plant computer engineers.

2. Unawareness of Software Security Patch

The plant computer engineering personnel had not been aware of the security patch that Microsoft released on July 10, 2002, to fix the Microsoft SQL Server 2000 vulnerability that the MS SQL worm exploited. In addition, on January 25, 2003, Microsoft issued an alert about the MS SQL worm. On the same day, CERT Coordination Center, a

federally funded research and development center that provides Internet security expertise, also issued Advisory CA-2003-04, MS-SQL Server Worm. A revision to this advisory was issued on January 27, 2003.

In response to this event, Davis-Besse implemented the following corrective actions:

(1) required network services to document all external connections to internal network, (2) installed the security patch for the MS SQL Server 2000 vulnerability, (3) installed a firewall between the plant network and the corporate network, (4) established a requirement to monitor and filter the data coming into the plant network to the same standard as the corporate firewall, and (5) implemented a process for computer engineering personnel to review security patches for systems supported and install them within an acceptable timeframe.

This information notice requires no specific action or written response. If you have any questions about the information notice in this notice, please contact one of the technical contacts listed below or the appropriate project manager in the NRC's Office of Nuclear Reactor Regulation (NRR).

/RA/

William D. Beckner, Chief
Reactor Operations Branch
Division of Inspection Program Management
Office of Nuclear Reactor Regulation

Technical contacts: Samuel S. Lee
(301) 415-1061
E-mail: ssl@nrc.gov

Matthew Chiramal
(301) 415-2845
E-mail: mxcc@nrc.gov

Eric J. Lee
(301) 415-8099
E-mail: exl@nrc.gov

Attachment: List of Recently Issued NRC Information Notices